

# **SECURITY IN DOE**

## ***A PROGRESS REPORT***



A Report to the Secretary of Energy  
From the  
Office of Security and Emergency Operations

January 2000

# SECURITY IN DOE: A PROGRESS REPORT

This past year the Department reacted decisively to the “wake up call” it received when major internal security problems were uncovered and by the publication of both the Cox and Rudman Reports. The Department was extremely close to losing the confidence and trust of both the American people and the Congress with respect to its ability to perform its security responsibilities. The enormous negative media coverage surrounding recent security-related events coupled with DOE’s historical track record of security deficiencies added to this erosion of public trust.

Over the years the Department lost its focus on security. On several occasions the Secretary has referred to the Department as being “a group of fiefdoms within fiefdoms” - and almost every fiefdom had its own security responsibility and security budget. There was no one office within the Department that had ultimate accountability for the critical security requirements for which DOE is responsible, nor was there any emphasis on individual accountability. This organizational dysfunction and lack of focus led to a deterioration of security awareness and education resulting in a failure to remind and educate our employees and contractors of their personal security responsibilities and accountability. There was a pervasive lack of attention to our cyber security practices in a world of increased computer hacking and cyber terrorism; and a gradual erosion of resources required to improve our capabilities to combat ever-changing terrorist and cyber terrorist threats. These common threads of inadequate protection practices had also been highlighted in more than twenty security reports, studies, and evaluations during the last decade. The Secretary directed an abrupt end to this unacceptable situation.

## **AN UNPRECEDENTED FOCUS**

In May 1999, Secretary Richardson announced his Security Reform Package - the most sweeping reform of security programs in the Department’s history. This comprehensive plan involved the creation of the Office of Security and Emergency Operations, the enhancement of the Office of Counterintelligence, and the elevation and revitalization of the Office of Independent Oversight and Performance Assurance. In the words of Secretary Richardson, “this plan gives DOE the tools and authority we need to detect security infractions, correct institutional problems and protect America’s nuclear secrets.”

In June 1999, Secretary Richardson asked General Eugene E. Habiger (U.S. Air Force, Retired) to become the Department’s “Security Czar” and he accepted the challenge. He was charged by the Secretary with changing the security culture at DOE and establishing a program to re-energize and restore confidence in the Department’s security program. As the “Security Czar,” he is responsible for implementing the Secretary’s security reform package and exercising management and direction of all security functions, including safeguards and security, cyber-security, critical infrastructure protection, foreign visits and assignments, and emergency operations.

The Office of Security and Emergency Operations, which was established in July 1999, also includes a single cyber security organization, under the direction of the Chief Information Officer.

A new Office of Plutonium, Uranium, and Special Materials Inventory was established that is responsible for maintaining real-time, reliable and complete information on DOE nuclear materials that are subject to special control and accounting procedures. Additionally, an Office of Foreign Visits and Assignments was formed to serve as a central accounting center to track and analyze the details of all foreign visits and assignments for all DOE facilities to ensure that these are conducted in a secure manner.

In order to strengthen General Habiger's ability to manage the responsibilities of his office, in August 1999 the Deputy Secretary directed that the DOE FY 2001 budget request include Safeguards and Security as a specifically identified, direct-funded activity within the new Office of Security and Emergency Operations. He also directed that all FY2001 Safeguards and Security funding in the budget of other Department organizations be identified and transferred to the Office of Security and Emergency Operations.

Department-wide operational "stand-downs" focused the Department's employees and contractors on their security responsibilities. On June 21-22, 1999, the Secretary directed a stand-down of Lawrence Livermore, Sandia, and Los Alamos National Laboratories, in order to carry out a two-day security immersion program. In April, all classified computers at these weapons labs were shut down for two weeks for security upgrades and worker training. Additionally, every DOE site with a National Security mission ceased work activities on August 3 for the entire day to participate in a program of security awareness and training. These "stand downs" have in fact increased awareness and improved the Department's security practices.

The foundation of the Secretary's security reform plan is his policy statement regarding security incidents and violations. In this statement, the Secretary established a standard of personal accountability by DOE employees and contractors for protecting DOE's national security assets. The Secretary further established a policy of "zero tolerance" for violations of security requirements that could place nuclear or other sensitive information at risk. This policy statement makes it clear that the Department is holding its people accountable . . . at all levels!

It is also clear that security, like safety, must become second nature in our day to day operations. Our workforce...both Federal and contractor...is the most critical link in the chain of protection of security interests. Consequently, the Department is instilling a sense of urgency and corporate ownership in all DOE employees and contractors, not just those that have security as part of their job descriptions. Efforts to ensure that employees are fully aware of their own individual protection responsibilities have been dramatically enhanced.

For those individuals whose primary duties relate to the protection of national security assets (that is, security professionals), a comprehensive career development initiative has begun that establishes a centrally managed competency based promotion and assignments program designed to institute staffing uniformity and enhanced operability throughout the complex. This initiative parallels similar successful programs in other government agencies, the military and private industry.

Based on this unprecedented focus by the Secretary on security, a real change is occurring in the Department culture... which will hopefully result in a positive momentum toward regaining that all-important special trust of the American people and Congress.

## **SPECIFIC INITIATIVES**

Through a series of comprehensive and sweeping initiatives, the Department has turned the corner and is aggressively and dynamically changing the way it does its security business. Soon after coming on board, General Habiger put in motion an intense, Four-Phased Security Campaign.

**Phase I**, which was completed in August, included visits by General Habiger to each of the major DOE sites in the field and established a baseline from which to move forward. He talked to thousands of DOE scientists and technicians to get their ideas and concerns first hand. Areas requiring immediate fixes were identified and corrective actions were taken – for example, the Department-wide security stand-downs, and issuing a policy for control of foreign visitors who visit our facilities to ensure that the tightest possible security procedures are followed.

**Phase II** was finished in December. It included the publication of policy addressing key issues, including the protective force carrying a round in the chamber of their weapon while on duty; foreign national access to cyber systems; badge validation procedures; and protection, generation and use of computer system passwords. This phase also included the development of a cross-talk program so that lessons learned could be shared across the Department.

**Phase III** began this month and will continue until March of 2000; by then most new policies addressing security issues will have been implemented. General Habiger will revisit the field to evaluate the effectiveness of the new or revised policies. At this stage, most of the major security deficiencies will be fixed and the focus will be turned to improvements and enhancements.

When we reach **Phase IV**, April to September of 2000, proposed security enhancements will be in effect and our efforts will turn toward adjustments as we maintain our security program. Critical activities will include scheduled visits to the field with continuous feedback and regularly conducted meetings with representatives from all sites to exchange lessons learned and best practices.

An integral part of every phase of this security campaign has been developing and refining a comprehensive set of metrics that can be used to measure the security program to ensure that we are making continuous improvements.

The following are major accomplishments of 1999, in the areas of safeguards and security, cyber security, and emergency operations.

### ***Safeguards and Security Accomplishments:***

- Standardized identification badges and vouching procedures.
- Established standard practices for divesting excess weapon inventories.

- Centralized the training for all new security police officers.
- Eliminated the backlog of personnel security clearance applications.
- Developed a new streamlined, more effective process to validate site security plans.
- Trained the way we protect . . . now all DOE sites with armed officers have live rounds in the chamber of their weapons.
- Mounted an aggressive and comprehensive security education and awareness campaign to remind each and every individual of their obligations. Developed an integrated security awareness training curriculum.
- Developed a new policy on Foreign Visits and Assignments.
- Conducted no-notice security checks at Headquarters and field facilities.
- Accomplished a short-notice audit of records of DOE employees enrolled in Personnel Security Assurance Program at three major field activities.

***Cyber Security Accomplishments:***

- Integrated unclassified and classified cyber security to make it a seamless program.
- Developed site specific computer security plans much like we do on the physical security side of the house.
- Trained approximately 700 system administrators Department-wide.
- Issued policy on generation, protection and use of passwords.
- Issued policy on foreign national access to DOE cyber systems.
- Issued policy requiring the use of warning banners on cyber systems.
- Established one central facility to respond to cyber attacks (the Computer Incident Advisory Capability at Lawrence Livermore National Laboratory). This team provides 24-hour a day monitoring.
- Purged DOE websites of sensitive information.
- Achieved Y2K success -- only 36 computer malfunctions out of over 200,000 systems.

***Emergency Operations Accomplishments:***

- Total reorganization . . . now leaner . . . more responsive.
- Aligned authority with responsibilities.
- Began aggressive new training and exercise programs.
- Designed one central DOE center to issue atmospheric information in the event of an accident or incident.

## **RESULTS AT THE WEAPONS LABORATORIES**

The National Laboratories have received the Secretary's message that security matters, and that they must pay attention to security and give it the appropriate priority as they conduct their normal business. Significant effort and resources has been devoted to correcting security deficiencies. Although security procedures are now being strictly enforced, workers are realizing that they can both do their jobs, and follow good security practices.

Positive results at Sandia include the relocation of classified weapons parts into areas or containers that enhance security for storing such parts, limiting access to unclassified computer systems by foreign nationals, and increased management focus on protective forces and security equipment issues. Additionally, Sandia has one of the most effective cyber security programs in the Department.

At Los Alamos some of the improvements include increased protective force staffing, revised and tested response plans and improved protective force training. Additionally, new security systems hardware has been purchased and installed to address previous deficient findings, and a security system upgrade line item is in progress. Los Alamos is now recognized as having the best special nuclear materials control and accountability programs within DOE.

Livermore has made significant progress towards correcting identified deficiencies. Improvements include the purchase of new measurement equipment for nuclear material, physical security and electronic systems have been upgraded and new equipment added. Additionally, significant major improvements have recently begun with the protective force by adding personnel and reestablishing the Special Response Team capacity. Livermore has one of the most difficult physical security problems in the Department and they are responding aggressively and effectively to meet this challenge.

In the cyber security area, the Office of Security and Emergency Operations has seen increased positive initiatives by information technology management at all three weapons laboratories. The Chief Information Officers at the laboratories have been involved in developing integrated security management for cyber security. The weapons laboratories have been proactive in training system administrators and have been aggressive in developing security program plans for their unclassified systems.

## **WHAT'S LEFT TO BE DONE**

We have taken monumental strides toward improving security; however, there is still work to be done. The following items highlight activities that the Office of Security and Emergency Operations will aggressively pursue this year.

- Disseminate policy to standardize the procurement of firearms, chemical protection equipment, communications equipment, body armor and armored vehicles.
- Develop common security and condition codes to ensure a standardized and coordinated response across the Department to changing terrorist threats.
- Combine two separate and distinct Human Reliability Programs within the Department into one -- taking the best aspects of each.
- Complete transition to a more effective force-on-force simulation model that will allow better employ of security forces.

- Develop a common strategy for the Department regarding explosive detection capabilities.
- Complete ongoing programs to ensure physical incompatibility between classified and unclassified computer systems as well as totally restricting any capability of removing data from a classified system.
- Develop a comprehensive cyber security architecture.
- Train and exercise realistically, the way DOE would be expected to function during a national security emergency.

## **SUMMARY**

Today, the Department of Energy functions in a security environment decidedly different from the one we faced a decade earlier. There is growing concern about a new breed of asymmetric threats that confront DOE and the Nation's security structures. Terrorism, Weapons of Mass Destruction and cyber attacks on information systems have become ingrained in the global psyche and in the Nation's security consciousness. These non-traditional, multi-directional threats test security resolve and capabilities as never before.

We cannot directly control or alter the threats to the security interests entrusted to our care. What can be controlled, however, is our ability to plan and respond to these threats should they ever materialize. The changing security environment and other threats over the past decade have fundamentally altered the Department's security perspective and posture. This is a significant challenge, but one that the Department of Energy must be prepared to meet.

The Department of Energy has made significant progress over the past year in standing up a new security organization with the authority and full backing of the Secretary to make things happen. The support, cooperation and buy-in of the dedicated members of the DOE team of scientists, technicians, and support personnel are unequivocal. These professionals are committed to continued excellence and serving their country in an environment that produces the very best science within a framework of security that is effective, but not unjustifiably intrusive. The American people and Congress will accept nothing less.